Assessing Privacy Awareness from Browser Plugins

Aditya Marella, Chao Pan, Ziwei Hu, Florian Schaub, Blase Ur, Lorrie Faith Cranor
School of Computer Science
Carnegie Mellon University
{amarella, chaop, ziweih, fschaub, bur, lorrie}@cmu.edu

1. MOTIVATION
The rise of social networking platforms and Internet connected smartphones has increasingly exposed user’s personal information. People generate and disclose vast amounts of personal information without being aware about what is being collected or who is collecting it. Malandrino et al. [4] have shown that making people aware of privacy risks could lead them to take steps to protect their privacy. Leon et al. [3] have examined the usability aspects of browser privacy plugins, they have also evaluated [2] what online behavioral advertising disclosures communicate to users. Balebako et al. [1] studied the effectiveness of privacy tools for limiting behavioral advertising. In this preliminary study, we explore the effectiveness of a placebo tool and three browser privacy plugins – Ghostery, Disconnect and DoNotTrackMe – in communicating awareness about privacy risks to users.

2. METHODOLOGY
We performed a between-subjects lab study with twelve participants in an interview setting. Each participant was randomly assigned one of four tools: Ghostery, DoNotTrackMe, Disconnect, and PrivacyGuard. The first three are existing privacy plugins available for Firefox and Chrome. While PrivacyGuard is a placebo tool without any functionality included as a control group.

Our lab sessions consisted of two phases. In the first phase, each participant completed searching and viewing tasks on four websites (amazon.com, nytimes.com, veoh.com and shop.com) without a privacy plugin. They were asked to rate the websites on a 7-point Likert scale based on how concerned or unconcerned they were about their privacy. Next, participants were asked to install the assigned privacy plugin. They were not provided with additional information beyond the plugin description. We instructed participants to familiarize themselves with the plugin. In other words, we tested the best case scenario in which the user explicitly attempts to read and understand how the plugin works.

In the second phase, participants were asked to perform similar but slightly different tasks on the same four websites. After each task, they rated the website again based on how concerned or unconcerned they were about their privacy. If they changed their rating they were asked to explain their reasons. By observing the change in the rating before and after installation of the plugin, we hope to understand the awareness gained by using the tool. After completion of the tasks, participants were asked general (non-task specific) questions to understand whether the plugin was effective in changing their privacy perception on the shown websites.

Control Group.
A fourth of the participants were assigned to a placebo tool in order to understand whether changes of rating are due to a psychological feeling of safety caused by the plugin. We developed a plugin (PrivacyGuard) which claims to protect user privacy but really did not have any functionality. The PrivacyGuard UI is shown in the right-most image in Figure 1. The plugin’s UI has been designed to state nothing about tracking or targeted advertising. In fact it does not give any information about the plugin, beyond stating that it protects the user’s privacy online.

3. RESULTS
About 50% of participants ended up changing their rating after using the assigned privacy plugin. We observed that Ghostery was very effective (100% changed rating) in making the participants change their rating whereas DoNotTrackMe was more effective (58%) in making users more concerned about their privacy. Disconnect was as effective as DoNotTrackMe in making the participants change their rating. Table 1 provides an overview of how ratings changed.

<table>
<thead>
<tr>
<th>Website</th>
<th>GH</th>
<th>DNTMe</th>
<th>DIS</th>
<th>PG</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>3/0/0</td>
<td>0/2/1</td>
<td>0/2/1</td>
<td>0/2/1</td>
<td>3/6/3</td>
</tr>
<tr>
<td>Veoh</td>
<td>2/1/0</td>
<td>0/2/1</td>
<td>1/2/0</td>
<td>0/3/0</td>
<td>3/8/1</td>
</tr>
<tr>
<td>Nytimes</td>
<td>1/2/0</td>
<td>0/2/1</td>
<td>2/0/1</td>
<td>0/2/1</td>
<td>3/6/3</td>
</tr>
<tr>
<td>Shop</td>
<td>2/1/0</td>
<td>1/1/1</td>
<td>0/1/2</td>
<td>2/1/0</td>
<td>5/4/3</td>
</tr>
<tr>
<td>Total</td>
<td>8/4/0</td>
<td>1/7/4</td>
<td>3/5/4</td>
<td>2/8/2</td>
<td>14/24/10</td>
</tr>
</tbody>
</table>

Table 1: Changes in privacy concern ratings for each website after using the privacy plugins (more concerned / less concerned / no change).

We observed that the reasons for changing concern ratings fall into the following categories. Note that the actual reason could be a combination of multiple categories.

Number of trackers: participants became both less and more concerned when they saw more trackers on the websites. The extent of concern depended on their surprise level and prior knowledge. Some participants were less concerned because the plugin was blocking the trackers while others became more concerned because they did not think that so many trackers would be tracking them on seemingly innocuous and popular websites, such as nytimes.com.

Popularity of website: popularity of the website had a huge negative impact on the rating change. Participants were reluctant to change their rating on the popular web-
sites amazon.com and nytimes.com. Even though veoh.com had less number of trackers than nytimes.com participants expressed less concern for nytimes.com than for veoh.com. Participants were most concerned about shop.com because it had lots of trackers and was not well known.

Placebo effect and control group: interestingly, 66% of the participants became slightly less concerned after installing the placebo plugin, although they were not sure if the tool was doing anything to protect their privacy. One participant noticed lots of advertisements and popups even after installation of the plugin and decided to keep the rating same during the last task.

Nature of task: a couple of participants changed the rating based on the search term or the type of product they were viewing. One participant found the search term ‘Obama’ to be more sensitive than ‘business.’ The same participant reported that she was not at all concerned when she searched for ‘bottled water.’

Trackers from obscure companies: participants expressed more concern when they saw trackers from unknown companies. They noticed this difference when they compared trackers on amazon.com with shop.com. They felt more comfortable on amazon.com not only because it had less number of trackers but also because the trackers were from well known reputable companies.

4. DISCUSSION
We found that only 11% of the participants gained any knowledge about the data collection and sharing practices of the trackers from the plugin and none of the participants were clear about the privacy risks associated with the data collection. Ghostery was most effective in improving awareness about data collection and sharing.

The purpose of data collection and sharing was unclear to most of the participants, 60% of participants were not sure about the purpose. The remaining participants stated marketing, advertising, recommendations and political agenda as the purpose. Among them only 11% changed their answer from not sure to advertising after using the tool.

All the plugins were reasonably effective in communicating sharing targets. 30% of the participants changed their answer on sharing targets from ‘not sure’ to the ‘tracking companies’ shown by the plugins. Interestingly, participants started speculating about sharing targets based on the search terms or the type of task they were performing.

78% of the participants did not believe they derived any benefit from the data collection. The remaining participants mentioned recommendations as the benefit.

Participants also perceived privacy risks differently for different categories of websites (retail, news and video). Of the participants, 25% believed video websites, 33% believed retail websites, and 17% believed news websites pose the highest privacy risks.

Overall, we found that participants changed their ratings not only because of the information shown by the plugin but also because of their pre-conceived notions and sometimes because of misconceptions. Given more exposure to the plugin, it is likely that users would be able to figure out the sharing targets and also the difference between a placebo tool and a real tool.

5. CONCLUSION
In summary, our work gives a perspective on privacy awareness gained by using browser privacy plugins. We plan a followup study with more participants that will allow us to probe deeper into what features of browser plugins successfully raise privacy awareness and how these tools may be further improved.

6. REFERENCES